(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 October 2004 (07.10.2004)

PCT

(10) International Publication Number
WO 2004/086664 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number:
PCT/IL2004/000144

(22) International Filing Date: 16 February 2004 (16.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

155121	27 March 2003 (27.03.2003)	IL
156950	15 July 2003 (15.07.2003)	IL

(71) Applicant *(for all designated States except US)*: **NDS LIMITED** [GB/GB]; One London Road, Staines, Middlesex TW18 4EX (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BELENKY, Yaacov** [IL/IL]; 27/2 Hakinor Street, Maaleh Adumim 98371 (IL). **SHEN-ORR, Chaim, D.** [IL/IL]; 16 Kiryat Sefer Street, Haifa 34676 (IL).

(74) Agents: **SANFORD T. COLB & CO.** et al.; P.O. Box 2273, Rehovot 76122 (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: IMPROVED CFM MODE SYSTEM

(57) Abstract: A method for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K, the method including receiving n plaintext blocks, wherein n is an integer greater than 0, setting Q_0 equal to an initial value, and for each plaintext block of the n plaintext blocks: computing $Q_i = E_K(Q_{i-1})$ *XOR* P_i; and computing $C_i = M(P_i, Q_i)$, thereby producing n ciphertext blocks, wherein $0 < i \leq n$, and P_i denotes an i-th plaintext block of the n plaintext blocks, and C_i denotes an i-th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted. Related apparatus and methods are also provided.

WO 2004/086664 A2